by reference. Generally, the present invention relates to a system and method for securely linking computers using an intelligent token. In U.S. Pat. No. 5,448,045, a computer is securely booted directly from an intelligent token and the computer is authenticated to the intelligent token. The present invention, in addition to the secure boot, provides the user with access to a remote domain including a remote host computer using the intelligent token. That is, the present invention authenticates the user and the intelligent token to the remote host computer without the necessity of the user inputting additional authentication information. Referring to FIG. **1**, for example, the intelligent token (not shown) may be coupled with a local host computer **30** and the local host computer **30** may be coupled to the remote domain **50**. The present invention allows the user to 1) securely boot the local host computer **30** and 2) authenticate the intelligent token **10** to the remote host computer **52** and, thus, to the remote domain **50** to allow free communication back and forth between the local host computer **30** and the remote domain **50**.

In accordance with the invention, as shown in FIG. **2**, the intelligent token **10** includes an IC (integrated circuit) **11** having a CPU **12** and a memory **14**. The memory **14** includes a ROM **16** and an EEPROM **18**. As depicted in FIG. **3**, the intelligent token **10** stores a protected copy of the file that is usually stored in a disk boot sector of a computer along with other file integrity data. The ROM **16** preferably stores the operating system of the intelligent token **10**. The EEPROM **18** preferably stores software programs to enforce access control to the host computer and access control to the remote domain **50** (access control software **20**). For example, the EEPROM **18** may include software that generates a request for access to the remote host computer **52** as well as software that generates responses to challenges sent by the remote host computer **52**. In addition, critical information such as boot sector information **22**, file integrity information **24** and authentication information **26** may be stored in the EEPROM **18**. The authentication information may include, e.g., file signature information and cryptographic keys for both the host and remote computers. Also, other sensitive or private information may be stored to ensure its integrity such as a remote access code for the remote host computer.

Traditionally, the above described critical information has been stored in the host computer's boot-sector memory. However, it is desirable to store as much information as possible on the intelligent token **10**. Of course, the amount of memory available in the intelligent token **10** will dictate the amount of data which may be stored there.

In a preferred embodiment, the intelligent token **10** may be a smart card marketed under the trade designation MCOS32k by Gemplus International. The International Standards Organization (ISO) defines a smart card as a credit card sized piece of plastic having an embedded IC. While the MCOS32k is particularly preferred, several chip vendors including SGS Thompson, Datakey and Toshiba provide IC's for use with intelligent tokens in the form of smart cards, keys and PCMCIA cards that may be used with the instant invention. In general, these vendors have employed micro-controllers in their IC's with clock rates much lower than typical desktop computers. These IC's are used in smart cards and other intelligent tokens. However, higher performance chips are under development.

The host computer is preferably an IBM or IBM compatible PC. Accordingly, as illustrated in FIG. **4**, the host computer **30** preferably includes a central processing unit (CPU) **32** connected to a memory **34**. The host computer may also include a hard disk drive **36** and a floppy disk drive **38**. Preferably, the host computer has a modified boot program. On a PC, for example, this may be realized by a modification of the BIOS or by addition of an add-in board **42** with a BIOS extension. Configuration software and file signature software are provided with the host computer. A reader/writer **40** for the intelligent token **10** is preferably coupled to the host computer. The reader/writer is preferably a smart card drive. The add-in board **42** (or modified BIOS) contains additional memory in the form of a special boot PROM which is loaded with a modified boot program which interfaces to the reader/writer. Further, the add-in board is configurable to set an identifier for the host.

The remote domain **50** may consist of a remote host computer **52**. The remote host computer **52** preferably has a basic construction similar to the local host computer **30**. However, the remote host computer **52** may also include a challenge generator that generates challenge signals responsive to a request for access to the remote computer **52**. The challenge generator may be implemented in hardware or software. An exemplary challenge generator is a random number generator. The remote host computer **52** may store validation information in its memory to validate responses emanating from the intelligent token **10**.

The remote domain **50** is not limited to a single remote host computer. The remote domain **50** may consist of a network including the remote host computer **52** and other computers **54**. For example, the remote domain **50** may include a network such as the Internet, and the remote host computer **52** may be a firewall.

As explained in U.S. Pat. No. 5,448,045, during system start up, two authentications must be successfully performed to complete the boot sequence. First, the user must be authenticated to the intelligent token **10** (user authentication) and, second, the intelligent token **10** must be authenticated to the host (host authentication). To authenticate the user to the intelligent token **10**, the user enters a password to the reader/writer. The intelligent token **10** checks the password to confirm that the user is authorized to use the intelligent token **10**. If successful, the intelligent token **10** allows the host computer to read the boot sector and other information from the intelligent token memory. To authenticate the intelligent token **10** to the host, the intelligent token **10** must also make available a secret shared with the local host **30** (a local secret) such as a configurable host identifier. If both the user and card authentication are successful, the boot sequence completes, and control is given to the host computer operating system—some or all of which has been retrieved from the intelligent token **10**. The user may then proceed to utilize the host computer in the usual fashion, uploading additional information, i.e., applications or application integrity information from the intelligent token **10** as needed.

Refer now to FIGS. **5** and **6**, which show the control flow of the of the modified boot sequence from the point of view of the local host computer **30** and the intelligent token **10**, respectively. The flow diagram in FIG. **5** shows the control flow of the modified boot program loaded from the BIOS extension add-in card in the original boot sequence. FIG. **6** shows the processing that occurs during the boot sequence on the CPU **12** of the intelligent token **10** while it is in the intelligent token reader/writer **40**.

Turning to FIG. **5**, the modified boot program (BIOS extension) prompts the user for a password at step **60**. The user inputs a password and the password is read in step **62**. In step the password is sent to the intelligent token **10**. At the same time, as illustrated in FIG. **6**, the intelligent token **10**